UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

THOMAS LEFFLER, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. UBER TECHNOLOGIES, INC., UBER USA, LLC, and RAISER, LLC, Defendants.	Case No.: 18-cv-13 **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

INTRODUCTION

1. This class action seeks redress for negligence, intentional misrepresentation, breach of contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment.

JURISDICTION AND VENUE

2. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

3. The Court has personal jurisdiction over Defendant because Plaintiff's claims arise out of Defendant's contacts with Wisconsin.

4. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

PARTIES

5. Plaintiff Thomas Leffler is an individual who resides in the Western District of Wisconsin (Dane County).

6. Defendant Uber Technologies, Inc. ("Uber") is a Delaware corporation headquartered in San Francisco, California.

7. Defendant Uber USA, LLC is an affiliate of Uber Technologies, Inc. and is a Delaware limited liability company with its principal place of business in San Francisco, California.

8. Defendant Rasier, LLC is an affiliate of Uber Technologies, Inc. and is a California limited liability company with its principal place of business in San Francisco, California.

FACTS

9. Defendant Uber Technologies, Inc. is a global ride share company operating in more than 600 cities worldwide.

10. Around October of 2016, hackers accessed Uber user data stored on a third-party cloud-based service ("Security Breach"). The Security Breach disclosed the personal information of approximately 600,000 drivers (including license information); and names, email addresses, and private cell phone numbers for 57 million customers ("Private Information").

11. Upon information and belief, rather than comply with its obligations to disclose such breaches and inform the public and regulators of what occurred, Uber paid the hackers behind the breach $100,000 in exchange for the criminals' silence and assurance that they would delete the data. Uber covered up the payment by calling it a bug bounty, a legitimate payment to

third parties to stress test the security of their systems. Uber continued to fail to inform affected consumers of the Security Breach for more than one year.

12. Uber ultimately disclosed the Security Breach to the public on November 21, 2017. On November 22, 2017 Uber also filed a notice of the Security Breach with the Wisconsin Department of Agriculture, Trade & Consumer Protection.

13. The Security Breach was not the first evidence of Uber's disregard for customer privacy. On November 19, 2014, Uber founder Travis Kalanick received a letter from Senator Al Franken stating that Uber had a "troubling disregard for customer privacy" and that "it appears that on prior occasions [Uber] has condoned use of customers' data for questionable purposes."

14. On February 27, 2015, Uber announced that it suffered a data breach nine months previous, including the names and license plate numbers for approximately 50,000 drivers. Uber waited more than five months after discovering this breach to notify the people affected.

15. In August of 2017, Uber entered into a settlement with the Federal Trade Commission admitting to making false claims about the privacy of consumer data and to maintaining inadequate safeguards to protect consumer data.

16. Plaintiff has been a user of Uber's services since about September of 2014.

17. On information and belief, Plaintiff's cell phone number, name, and email address were compromised in the Security Breach.

18. Private Information is a valuable commodity to identity thieves. Once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

19. The value of Plaintiff's and Class members' Private Information on the black market is substantial. By way of the Security Breach, Uber has deprived Plaintiff and Class members of the substantial value of their Private Information and opened Uber users and their private phone numbers to nefarious elements of society and their disruptive tactics, including unwanted phone calls.

20. Uber's conduct demonstrates a willful and conscious disregard for consumer privacy. The Security Breach has exposed the private information of Plaintiff and approximately 57 million other users of Uber's service. Rather than take steps to inform the public of what occurred, Uber allegedly paid criminals in an effort to conceal the Security Breach.

COUNT I - NEGLIGENCE

21. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

22. Defendant owed to Plaintiff and the other Class members a duty to exercise reasonable care in handling and using personal information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from theft or unauthorized use and detect attempts at unauthorized access.

23. Additionally, under Wis. Stat. § 134.98, Defendant owed to Plaintiff and the other Class members a duty to notify them within a reasonable timeframe of any breach to the security of their personal information.

24. Defendant owed these duties to Plaintiff and the other Class members because Plaintiffs and the other Class members are a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited Plaintiff and the other Class

members' personal information. Plaintiff and the other Class members were required to provide their personal information to Defendant in order to obtain services, and Defendant retained the information throughout the Plaintiffs' and other Class members' use of Defendant's services.

25. The risk that unauthorized persons would attempt to gain access to the personal information was foreseeable. As an aggregator of vast amounts of consumer data, it was inevitable that unauthorized individuals would attempt to access Defendant's databases of personal information. Such information is valuable, and numerous instances of criminal attempts to access this kind of information have been publicized. In fact, Defendant has been targeted successfully in the past by such attempts. Defendant knew, or should have known, the risk in obtaining, using, handling, and storing the personal information of Plaintiff and the other Class members, and the importance of exercising reasonable care in handling it.

26. Defendant also owed a duty to timely and accurately disclose to Plaintiff and the other Class members the scope, nature, and occurrence of the Security Breach. This duty was required and necessary in order for Plaintiff and the other Class members to take appropriate measures to protect their information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Security Breach.

27. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information of Plaintiff and the other Class members, which proximately caused the Security Breach and Plaintiff's and the other Class members' injuries.

28. Defendant breached its duties by failing to provide timely and accurate notice of the Security Breach to Plaintiff and the other Class members, which proximately caused and exacerbated the Security Breach, and Plaintiff's and the other Class members' injuries.

29. Defendant's failures and negligence proximately caused Plaintiff and other Class members to suffer the theft of their personal information by criminal actors and actual damages including the improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and breach of common law duties to exercise reasonable care, including the increased risk of identity theft that resulted and continues to face them.

COUNT II - INTENTIONAL MISREPRESENTATION

30. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

31. Defendant knowingly made false and deceptive representations regarding its data security practices and policies, in its privacy statement and elsewhere, including enumerating specific uses and ways in which the information could be shared.

32. Defendant additionally knowingly made false and deceptive statements to cover up and conceal the Security Breach through knowing misrepresentations and omissions of material fact. Defendant knowingly misrepresented the ransom paid to the hackers, and falsely labeling it a bug bounty. Defendant omitted the material fact that the ransom was actually paid to hackers who had executed the Security Breach.

33. These knowing misrepresentations were intended to conceal and delay the notification of and the investigation into the Security Breach for more than a year in order to induce the public to enter into a contract for Defendant's services and/or increase consumption of Defendant's services.

34. As a result of Defendants false statements, Plaintiff and the other Class members continued to use Uber's services and have suffered additional pecuniary loss, including improper

disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT III - BREACH OF CONTRACT

35. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

36. Defendant entered into a contract with Plaintiff and the other Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class members' personal information.

37. Plaintiff and the other Class members bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their personal information.

38. Plaintiff and the other Class members performed their duties under the agreements.

39. Defendant violated the terms of the contract in the Security Breach by sharing Plaintiff's and the other Class members' personal information for unauthorized purposes, without first obtaining Plaintiff's or the other Class members' consent or anonymizing and/or aggregating the information in a form which cannot reasonably be used to identify them, and otherwise violating the terms of the contract.

40. Defendant violated the terms of the contract in the Security Breach by failing to take appropriate measures to protect Plaintiff's and the other Class members' personal information in accordance with its promises and representations. Defendant violated the agreement by failing to comply with applicable laws during the Security Breach regarding the access, correction, and/or deletion of personal data, and notification to affected persons.

41. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT IV - BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

42. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

43. The law implies a covenant of good faith and fair dealing in every contract.

44. Defendant entered into a contract with Plaintiff and the other Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class members' personal information.

45. Plaintiff and the other Class members performed their duties under the agreements.

46. Defendant's unlawful and bad faith conduct, as described above, constitutes a breach of the implied covenant of good faith and fair dealing.

47. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT V - UNJUST ENRICHMENT

48. Plaintiff pleads this count in the alternative and incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

49. Plaintiff and the other Class members conferred a monetary benefit on Defendant in the form of money paid for the purchase of services from Defendant.

50. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiff and the other members of the Class.

51. Defendant knew about the Security Breach, its own deficiencies in security practices that caused it, and its own course of conduct in covering it up through false and misleading statements and omissions.

52. It would be inequitable for Defendant to retain these benefits.

53. There is no adequate remedy at law.

54. Plaintiff and the other Class members are therefore entitled to restitution, disgorgement, and imposition of a constructive trust.

CLASS ALLEGATIONS

55. Plaintiff brings this action on behalf of a Class, consisting of all natural persons in the United States whose private information was accessed by third parties in the October 2016 Uber data breach. Excluded from the Class are governmental entities, Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. The Class is so numerous that joinder is impracticable. Upon information and belief, there are more than 50 members of the Class.

57. There are questions of law and fact common to the members of the class, which common questions predominate over any questions that affect only individual class members.

58. Plaintiff's claims are typical of the claims of the Class members. All are based on the same factual and legal theories.

59. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff has retained counsel experienced in consumer credit and debt collection abuse cases.

60. A class action is superior to other alternative methods of adjudicating this dispute. Individual cases are not economically feasible.

JURY DEMAND

61. Plaintiff hereby demands a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendants for:

(a) actual damages;

(b) statutory damages;

(c) punitive damages;

(d) injunctive relief;

(e) attorneys' fees, litigation expenses and costs of suit; and

(f) such other or further relief as the Court deems proper.

Dated: January 8, 2018

ADEMI & O'REILLY, LLP

By: /s/ Mark A. Eldridge
Shpetim Ademi (SBN 1026973)
John D. Blythin (SBN 1046105)
Mark A. Eldridge (SBN 1089944)

3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com
jblythin@ademilaw.com
meldridge@ademilaw.com